

# UNITED STATES DISTRICT COURT

for the  
Eastern District of Missouri

**FILED**  
**MAR 04 2022**  
U.S. DISTRICT COURT  
EASTERN DISTRICT OF MO  
ST. LOUIS

In the Matter of the Search of  
INFORMATION ASSOCIATED WITH  
ROBERTSCOTTMASON2022@GMAIL.COM THAT IS STORED AT  
PREMISES CONTROLLED BY GOOGLE, LLC.

Case No. 4:22-MJ-05053-NAB

SIGNED AND SUBMITTED TO THE COURT FOR  
FILING BY RELIABLE ELECTRONIC MEANS

## APPLICATION FOR A SEARCH WARRANT

I, Ryan Cornelius, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

located in the NORTHERN District of CALIFORNIA, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

*Code Section - Offense Description*

Title 18 United States Code Section 2261A (Online Stalking)

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing is true and correct.

/s/ Ryan Cornelius  
Applicant's signature

Ryan Cornelius, Special Agent  
Printed name and title

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedures 4.1 and 41.

Date: 03/04/2022

Nannette A. Baker  
Judge's signature

City and state: St. Louis, MO

Honorable Nannette A. Baker, U.S. Magistrate Judge  
Printed name and title

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH  
ROBERTSCOTTMASON2022@GMAIL.COM  
THAT IS STORED AT PREMISES  
CONTROLLED BY GOOGLE, LLC.

Case No. 4:22-MJ-05053-NAB

SIGNED AND SUBMITTED TO THE  
COURT FOR FILING BY RELIABLE  
ELECTRONIC MEANS

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Ryan Cornelius, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by Google, LLC, an email provider headquartered in Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google, LLC to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a currently employed as a Special Agent of the Federal Bureau of Investigation, United States Department of Justice. I have been employed as a Special Agent of the Federal Bureau of Investigation since 2011. Prior to employment by the Federal Bureau of

Investigation, I was a licensed police officer since 2004. I have participated in numerous investigations which resulted in the seizure of evidence including controlled substances, firearms, paper records, electronically stored records, and electronic devices. I am familiar with and have utilized normal methods of investigation, including, but not limited to, physical and electronic surveillance, questioning of witnesses and suspects, the use of search and arrest warrants, controlled purchases of evidence, and the use of informants. I received training from the Federal Bureau of Investigation and other sources on the investigation of violations of United States code, the use of informants, the apprehension of criminal offenders, and the collection of evidence.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other investigators and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18 United States Code Section 2261A (Online Stalking) (hereinafter referred to as “the subject offense”) have been committed by **ROBERT DAVE PAUL MERKLE**. There is also probable cause to search the information described in Attachment A for evidence of these crimes, as described in Attachment B.

#### **JURISDICTION**

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), &

(c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

**PROBABLE CAUSE**

6. The Federal Bureau of Investigation is conducting an investigation involving threatening communications, threats of violence, and cyberstalking in violation of Title 18 United States Code Section 2261A, within the Eastern District of Missouri.

7. On January 27, 2022, your affiant was contacted by the Town and Country Missouri Police Department regarding a report of harassment and stalking which occurred within their venue.

8. On January 26, 2022, the Town and Country Police Department responded to an address in their venue and interviewed a complainant, identified as T.B. T.B. is known to investigators and is a live person.

9. T.B. reported she met **ROBERT DAVE PAUL MERKLE**, hereinafter referred to as **MERKLE**, on or about April 2014. T.B. reported she met **MERKLE** on a dating website and they had an intimate relationship. T.B. told investigators she broke up with **MERKLE** because he began exhibiting behavior T.B. considered threatening, such as choking during intercourse.

10. T.B. told investigators that during intermittent periods from 2014 through January 2022, T.B. continued to receive text messages from **MERKLE** which were annoying, but she did not consider them threatening. T.B. told investigators she ignored the text messages and did not respond to him.

11. T.B. told investigators that during the evening of January 26, 2022, she received a text message string from **MERKLE**, who she believed was using a fictitious or internet-generated telephone number. T.B. told investigators that although **MERKLE** was using an unfamiliar

telephone number, she knew it to be him because he referenced a nickname only he used, he described a specific attribute of her home, and he said they had sex during April 2014.

12. A transcript of the text messages investigators believe were sent by **MERKLE** is included below. T.B. told investigators she did not reply to the text messages.

- a. Hey Tamster?
- b. Remember the last night we had sex in late April 2014?
- c. I photographed your house key before we left your place that evening
- d. See there was this online company that made a physical copy of a key purely from a cellphone picture.
- e. Cool, ya know?
- f. I remember you looked at your keys on your breakfast bar table. You saw they had been moved and for a second I thought you were gonna sniff me out. But you never made the connection
- g. I got the key to your front door not but 5 fuckin days later
- h. And it worked, too [face emoji]
- i. I still have it and I bet the lock is still the same
- j. I'm gonna find out for sure this Friday nite, Tamster.
- k. So if you happen to wake up Friday nite around midnight w a hand over your mouth and a dick going in and out of your cunt, well, at least you'll know who it is
- l. Just like old times Tammy....just like old times

13. After the police arrived at the residence of T.B., she received a text message from who she believed was **MERKLE**. A transcript of a portion of the message is included below:

a. And for Christ's sakes, Tammy, quit calling the fuckin cops on me. Now I'm gonna have to call in another favor w/ my...ummmm..."F"lowers "B"y "I"rene buddies to quash this shit

b. Damnit woman!

14. Investigators believe because when **MERKLE** was texting T.B. he knew of the police presence at her residence, **MERKLE** may have had an accomplice watching T.B., or a technical ability to track T.B. and her use of the phone. Investigators know because **MERKLE** previously worked in the information technology sector, he may have special knowledge of technical applications used to conduct cyber-related crimes.

15. Investigators asked T.B. if the key to her home had numbers at the top of it which correspond to the key cutting depths to make a new key. T.B. told investigators the key to her home has numbers on it. Your affiant believes the numbers on top of the key may have allowed **MERKLE** to easily make a duplicate key to her residence from only referencing an image.

16. On January 27, 2022, investigators, including your affiant, located **MERKLE** at his place of employment, located in the Eastern District of Missouri. Your affiant requested to talk to **MERKLE** and he refused to provide any substantiative information to law enforcement.

17. A Town and Country Police Officer arrested **MERKLE** for First Degree Harassment, a Class E State of Missouri Felony. A search of **MERKLE** did not locate any cellular telephones.

18. Investigators, including your affiant, learned that as **MERKLE** was walking from his work area to meet investigators at the front of the building, he gave an Apple iPhone to a coworker. Your affiant and another investigator interviewed the coworker **MERKLE** gave the Apple iPhone to and he told investigators he believed **MERKLE** gave the Apple iPhone to him

because **MERKLE** knew law enforcement was at the front and **MERKLE** did not want law enforcement to have the device. A Town and Country Police Department Detective seized the device. The phone was placed in “Airplane Mode” and the SIM card was removed and attached to the back of the device to prevent the device from being remotely altered or erased.

19. **MERKLE** was transported to the Town and Country Missouri Police Department where he was processed, photographed, and this matter was presented to the Office of the Saint Louis County Prosecuting Attorney. Charges were filed under cause number 22-SL-CR00573 and a bond was set at \$75,000.

20. On February 4, 2022 your affiant applied to the United States District Court for the Eastern District of Missouri for authorization to search **MERKLE’s** Apple iPhone and his apartment which were both located in the Eastern District of Missouri. United States Magistrate Judge Honorable Shirley Padmore Mensah authorized the searches and investigators subsequently seized multiple digital devices, including cellular phones, hard drives, and USB thumb drives from **MERKLE’s** apartment. The FBI began the process of forensic examination of the Apple iPhone on or about February 8, 2022.

21. On February 10, 2022 your affiant interviewed a female identified as J.A. She is a live person who is known to investigators. J.A. reported that prior to **MERKLE’s** most recent arrest by law enforcement, she received multiple emails from the email account: robertscottmason2022@gmail.com, hereinafter the **SUBJECT EMAIL ACCOUNT**.

22. J.A. reported to your affiant she received an unsolicited email sent on December 26, 2021 by the **SUBJECT EMAIL ACCOUNT** to her employer-provided email account. In the body of the document, the email read, “Hi Jenny, Didn’t you used to work on the 13<sup>th</sup> floor of WFA around 2014 or so? That’s when I was there. Private Client Group.”

23. J.A. told your affiant she worked in the referenced unit during 2014, but did not recognize the name “Robert Scott Mason.”

24. J.A. provided your affiant an email message sent from the **SUBJECT EMAIL ACCOUNT** on January 5, 2022 which read, “Yea. So anyway I remember you as being \*insanely\* smoking hot. Smoldering hot. In fact the first week or two after we started I recall you were wearing a micro (emphasis on micro) miniskirt, jacket, heels and tights. Don’t think I’ll ever forget that, Jenny. I thought: this girl must f\*ck like a g\*ddamn Ferrari.... And I’m proly not wrong in that analysis, wouldn’t you concur?”

25. J.A. provided your affiant an email message sent from the **SUBJECT EMAIL ACCOUNT** on January 16, 2022 which read, “Jenny I’d love to know your address. I like to masturbate and think about coming to your house sone night really late, getting in, mounting you with no grace at all and just start having really hard sex with you.”

26. J.A. provided your affiant an email message sent from the **SUBJECT EMAIL ACCOUNT** on January 17, 2022 which read, “Jenny what I’d really like to do is spray semen all over your face while you’re having an orgasm.”

27. J.A. told your affiant she consulted with a co-worker who worked in the same unit as she did during 2014 and identified people who were employed there during that time. J.A. told your affiant one party was identified as **MERKLE**. J.A. told your affiant she researched **MERKLE** on the Internet and thought he looked familiar, but she had few personal interactions with **MERKLE** during his time in that work unit.

28. Your affiant reviewed the email messages J.A. reported she received from the **SUBJECT EMAIL ACCOUNT** and observed the “From:” field displayed the **SUBJECT EMAIL ACCOUNT**.



29. A review of restricted law enforcement databases returned that **MERKLE** has a previous conviction for Harassment – First Degree, and arrests for Harassment – Second Degree, Domestic Assault, and Domestic Stalking.

30. A review of restricted law enforcement databases returned that **MERKLE** is the respondent in an active full order of protection. According to the terms of the order, **MERKLE** is restrained from assaulting, threatening, abusing, harassing, following, interfering or stalking the protected person. He is required to stay away from the protected person's residence, property, school, and place of employment. He is restrained from making any communication with the protected person, including personal written or telephone contact.

31. Your affiant reviewed police reports from the Saint Louis Metropolitan Police Department that showed that **MERKLE** was a suspect in similar previous incidents that occurred in 2017. In one report from April of 2017, a female victim identified Robert Merkle, with the same date of birth and social security account number as **MERKLE** identified in this matter, as a person who she met via an online dating application and whom sent her threatening and sexually explicit electronic messages.

32. In a September 2017 St. Louis Metropolitan Police report, Robert Merkle, with the same date of birth and social security account number as **MERKLE** identified in this matter, was identified as a suspect who reportedly sent the following messages to the victim who was an administrator of a section of an online dating website:

- a. "Currently I'm involved in the research of female sexual non-consensual sex acts (some of which do involve a moderate degree of sexual violence)"

- b. “I’m going to enjoy ejaculating into your vagina, my hand shoved down your throat, suffocating you while you try to scream, cumming your fucking goddamn brains out.”
- c. “I think you’re really pretty & I’m looking forward having non-consensual sex with you.”

33. On February 15, 2022 a preservation request was sent to Google, LLC. In general, an email that is sent to a Google, LLC subscriber is stored in the subscriber’s “mail box” on Google, LLC servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google, LLC servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google, LLC's servers for a certain period of time.

#### **BACKGROUND CONCERNING EMAIL**

34. In my training and experience, I have learned that Google, LLC provides a variety of on-line services, including electronic mail (“email”) access, to the public. Google, LLC allows subscribers to obtain email accounts at the domain name gmail.com, like the email account listed in Attachment A. Subscribers obtain an account by registering with Google, LLC. During the registration process, Google, LLC asks subscribers to provide basic personal information. Therefore, the computers of Google, LLC are likely to contain stored electronic communications (including retrieved and unretrieved email for Google, LLC subscribers) and information concerning subscribers and their use of Google, LLC services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute

evidence of the crimes under investigation<sup>1</sup> because the information can be used to identify the account's user or users.

35. A Google, LLC subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google, LLC. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

36. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

37. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the

account. In addition, email providers often have records of the Internet Protocol address (“IP address”) used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

38. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.

39. As explained herein, information stored in connection with an email account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as

described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

### **CONCLUSION**

40. Based on the forgoing, I request that the Court issue the proposed search warrant.


41. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google, LLC. Because the warrant will be served on Google, LLC, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

### **REQUEST FOR SEALING**

42. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the

targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

I state under the penalty of perjury that the foregoing is true and correct.

  
\_\_\_\_\_  
RYAN CORNELIUS  
Special Agent  
Federal Bureau of Investigation

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on this 4th day of March 2022.

  
\_\_\_\_\_  
NANNETTE A. BAKER  
United States Magistrate Judge

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with robertscottmason2022@gmail.com that is stored at premises owned, maintained, controlled, or operated by Google, LLC, a company headquartered at 1600 Amphitheater Parkway, Mountain View, California.

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Google, LLC (the “Provider”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on February 15, 2022 the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account beginning on August 1, 2021 to February 1, 2022, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. The contents of all chat or text messaging conversations associated with the account beginning on August 1, 2021 to February 1, 2022, including stored or preserved copies of chats or text message conversations sent to and from the account, draft chats or texts, the source and destination addresses associated with each chat or text message, the date and time at which each chat or text was sent, and the size and length of each chat or text;

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of



service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. The types of service utilized;

e. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

f. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within 14 days from the of issuance of this warrant.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18 United States Code Section 2261A those violations involving **ROBERT MERKLE** and occurring after August 1, 2021 including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Harassing, threatening and/or stalking communications;
- (b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

**CERTIFICATE OF AUTHENTICITY OF  
DOMESTIC RECORDS PURSUANT TO  
FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)**

I, \_\_\_\_\_, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by \_\_\_\_\_, and my title is \_\_\_\_\_. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of \_\_\_\_\_. The attached records consist of \_\_\_\_\_ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of \_\_\_\_\_, and they were made by \_\_\_\_\_ as a regular practice; and

b. such records were generated by \_\_\_\_\_ electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of \_\_\_\_\_ in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by \_\_\_\_\_, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature